EUROPEAN DATA PROTECTION SUPERVISOR

Lignes directrices relatives au traitement d'informations à caractère personnel dans le cadre d'une procédure d'alerte éthique

Juillet 2016

Résumé

L'alerte éthique a pour objectif de mettre en lumière les cas de corruption. L'un des grands aspects de la prévention et de la lutte contre la corruption est la détection et la mise à jour des pots-de-vin, fraudes, vols et autres actes répréhensibles commis sur le lieu de travail. L'alerte éthique est un outil visant à assurer la visibilité de ce type de comportements malhonnêtes.

Les lanceurs d'alerte estiment agir dans l'intérêt public lorsqu'ils signalent un fait grave dont ils ont été témoins. Malheureusement, ils sont régulièrement la cible de représailles, sous la forme de harcèlement, de licenciement, de mise sur liste noire ou de menaces, et leurs informations sont souvent ignorées. La confidentialité est donc essentielle et le moyen le plus efficace d'inciter les membres du personnel à signaler des problèmes est d'assurer la protection de leur identité.

Les présentes lignes directrices fournissent des orientations pratiques aux institutions et organes de l'UE, tant avant qu'après l'exécution d'une procédure d'alerte éthique, afin de s'assurer qu'ils respectent les obligations en matière de protection des données établies par le règlement (CE) n° 45/2001.

Liste des recommandations

Ci-dessous figure une liste des recommandations formulées dans les lignes directrices. Le Contrôleur européen de la protection des données (CEPD) s'en servira comme liste de contrôle pour évaluer votre respect des obligations énoncées dans le règlement.

1. Établir des filières spécifiques pour la soumission de rapports internes et externes ainsi que des règles spécifiques dont la finalité est clairement indiquée (pp. 4-5).

2. Assurer la confidentialité des informations reçues et protéger l'identité des lanceurs d'alerte ainsi que de toutes les autres personnes impliquées (pp. 4-5).

3. Appliquer le principe de minimisation des données: ne traiter que les informations à caractère personnel adéquates, pertinentes et non excessives pour l'affaire en cause (p. 6).

4. Déterminer ce que veut dire «information à caractère personnel» dans ce contexte ainsi que l'identité des personnes concernées, afin d'établir leur droit d'information, d'accès et de rectification. Les restrictions de ces droits sont autorisées pour autant que les institutions de l'UE soient en mesure de justifier au préalable leur décision (pp. 6-7).

5. Appliquer la procédure en deux étapes afin d'informer chaque catégorie de personnes sur la manière dont leurs données seront traitées (pp. 7-8).

6. Veiller, lors des réponses aux demandes relatives au droit d'accès, à ce qu'aucune information personnelle d'une autre partie ne soit divulguée (pp. 8-9).

7. S'assurer de la compétence du destinataire (interne ou externe), puis limiter le transfert d'informations à caractère personnel à ce qui est strictement nécessaire à l'exécution légitime des missions relevant de la compétence du destinataire (p. 9).

8. Définir des périodes de conservation adéquates pour les informations à caractère personnel traitées dans le cadre de la procédure d'alerte éthique, en fonction de l'issue de chaque cas (pp. 9-10).

9. Mettre en œuvre des mesures de sécurité organisationnelles et techniques, basées sur une analyse du risque de la procédure d'alerte éthique, afin de garantir le traitement sûr et licite des informations à caractère personnel (pp. 10-11).

TABLE DES MATIÈRES

1. INTRODUCTION

1 Les procédures de lancement d'alerte visent à fournir des filières sûres permettant à toute personne de signaler les cas potentiels de fraudes, corruptions et autres manquements et irrégularités graves dont elle a connaissance. Les lanceurs d'alerte estiment agir dans l'intérêt public lorsqu'ils signalent un fait grave qu'ils ont observé.

2 Le statut des fonctionnaires («le statut») et le régime applicable aux autres agents («le RAA»)[1] incluent l'obligation, pour les membres du personnel et les autres personnes qui travaillent pour les institutions et organes de l'UE («les institutions de l'UE»), de signaler par écrit toute suspicion raisonnable d'activités illégales à leur hiérarchie ou directement à l'Office européen de lutte antifraude («OLAF»). Certaines institutions de l'UE ont également adopté des règles internes sur le lancement d'alertes éthiques par leur personnel. Les dispositifs d'alerte éthique servant de mécanisme de détection lui-même destiné à signaler les cas d'activités illégales à l'OLAF, l'obligation d'information ne concerne que les manquements et irrégularités graves. La portée des présentes lignes directrices est limitée à l'étape initiale à laquelle les institutions de l'UE reçoivent une notification et ne couvre pas les cas où l'affaire est renvoyée vers l'OLAF ou directement transmise à celui-ci.

3 Les procédures d'alerte éthique supposent le traitement d'informations à caractère personnel. Les institutions de l'UE sont tenues de gérer les rapports d'alerte et de veiller à la protection des informations personnelles des lanceurs d'alerte, des présumés coupables, des témoins et de toutes les personnes apparaissant dans l'alerte. Les présentes lignes directrices expliquent comment appliquer les principes relatifs à la protection des données à ce contexte particulier, susceptible d'affecter la vie privée d'individus. Ces explications sont illustrées par une série d'exemples hypothétiques. Les lignes directrices montrent également que les principes relatifs à la protection des données peuvent servir à renforcer les procédures d'alerte éthique. L'application des principes relatifs à la protection des données favorisera notamment la création de filières sûres en renforçant les aspects de la procédure liés à la sécurité.

4 Les parties extérieures qui concluent un contrat avec les institutions de l'UE ou qui prennent contact avec celles-ci (p.ex. consultants, contractants, chercheurs, etc.) doivent être informées de la possibilité de signaler les suspicions de fraude, de corruption ou d'autres manquements et irrégularités graves.

5 Cette opération de traitement est susceptible de présenter des risques particuliers [2] et est donc soumise au contrôle préalable du Contrôleur européen de la protection des données («CEPD»).

[1] Le cadre juridique général applicable aux membres du personnel de l'UE agissant en tant que lanceurs d'alerte est établi aux articles 22 *bis*, 22 *ter* et 22 *quater* du statut, qui, conformément à l'article 11 du régime applicable aux autres agents de l'UE, s'appliquent par analogie aux agents engagés par contrat.
[2] Article 27, paragraphe 2, points a) et b), du règlement (CE) n° 45/2001 («lerèglement»).

2. DES FILIÈRES DE COMMUNICATION SÉCURISÉES POUR LE SIGNALEMENT DES FRAUDES - GARANTIR LA CONFIDENTIALITÉ

6 La manière la plus efficace d'inciter les membres du personnel à signaler leurs inquiétudes est de garantir la protection de leur identité. C'est pourquoi des filières de communication clairement définies pour les signalements internes et externes et la protection des informations reçues doivent être créées. L'identité du lanceur d'alerte signalant des manquements ou irrégularités graves en toute bonne foi doit être traitée avec la plus grande confidentialité afin de protéger le lanceur d'alerte contre d'éventuelles représailles. Son identité ne peut en aucun cas être révélée, hormis dans des circonstances exceptionnelles, s'il en autorise la divulgation, si cette dernière est requise par une procédure de droit pénale ultérieure ou lorsque le lanceur d'alerte fait une fausse déclaration par malveillance. Dans de tels cas, ces données à caractère personnel ne pourraient être divulguées qu'aux autorités judiciaires[3]. Une déclaration est effectuée par malveillance si le lanceur d'alerte signale des activités qu'il sait être inventées. Lorsqu'une institution de l'UE apprend qu'un lanceur d'alerte savait son allégation non fondée, il incombe à cette institution de démontrer le caractère malveillant des allégations.

7 La personne visée par une allégation doit être protégée au même titre que le lanceur d'alerte en raison du risque de stigmatisation et de victimisation de la personne au sein de l'organisation dont elle est membre. La personne sera exposée à ces risques avant même de savoir qu'elle a été mise en cause et avant même que les faits allégués aient fait l'objet d'une enquête pour déterminer s'ils sont fondés ou non.

8 Dès lors, l'accès en interne aux informations traitées dans le cadre de l'enquête sur les allégations doit être accordé sur la stricte base du principe du besoin d'en connaître, autrement dit, s'il existe une nécessité d'y accéder. Les personnes responsables de la gestion des rapports peuvent par exemple être soumises à une obligation de confidentialité renforcée. Les informations à caractère personnel doivent également être stockées en toute sécurité.

9 Toute information à caractère personnel en rapport avec une alerte éthique et conservée à des fins statistiques doit être rendue anonyme. Les institutions de l'UE (en particulier les plus petites) doivent être particulièrement prudentes avec les informations susceptibles de permettre une identification *indirecte*. Par exemple, enregistrer le type d'alerte éthique au même endroit que la nationalité du lanceur d'alerte pourrait entraîner l'identification indirecte de ce dernier et doit donc être évité.

Exemple 1: *une agence de l'UE a adressé des recommandations explicites à son personnel sur la manière d'assurer la confidentialité des lanceurs d'alerte et des présumés responsables lors de l'examen initial d'une affaire. Le CEPD souligne que la vulnérabilité des parties impliquées est la même, que l'affaire soit en cours ou qu'elle soit close. La protection des lanceurs d'alerte et des présumés responsables doit par conséquent être également prise en*

[3] Voir CEPD, dossier 2010-0458.

3. ÉVITER TOUT ABUS DE LA PROCÉDURE - SPÉCIFIER LA FINALITÉ

10 Le champ d'application de la procédure doit être limité afin d'éviter tout abus de la procédure. La finalité de la procédure d'alerte éthique doit être **clairement spécifiée**[4] dans le règlement intérieur ou la politique des institutions de l'UE. Le règlement interne ou la politique doit décrire expressément les circonstances dans lesquelles les filières de communication réservées aux alertes éthiques doivent être utilisées et les circonstances dans lesquelles elles ne doivent pas l'être. En règle générale, les filières de communication réservées aux alertes éthiques **ne doivent pas être utilisées** lorsque le membre du personnel pourrait souhaiter exercer ses droits légaux, à savoir introduire une demande ou une plainte auprès de l'autorité investie du pouvoir de nomination en vertu de l'article 90 du statut ou lorsqu'il s'agit d'un cas de harcèlement ou d'un différend personnel, auquel cas le membre du personnel peut s'adresser aux RH, au service de médiation ou à un conseiller qui respectera le principe de confidentialité, ou encore introduire une demande d'assistance au titre de l'article 24 du statut.

11 Le règlement intérieur ou la politique doit par ailleurs décrire les informations sensibles, telles que l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que les données relatives à la santé ou à la vie sexuelle[5], qui sont dénuées de pertinence pour l'affaire et qui doivent être évitées. Cela contribuera à éviter la collecte d'informations à caractère personnel excessives (voir ci-dessous).

12 En principe, **l'alerte éthique ne devrait pas être anonyme**. Les lanceurs d'alerte devraient être invités à s'identifier, non seulement pour éviter tout abus de la procédure, mais aussi pour permettre leur protection efficace contre d'éventuelles représailles. Cela permettra également une meilleure gestion du dossier dans le cas où des informations supplémentaires seraient nécessaires.

4. ÉVITER LE TRAITEMENT D'INFORMATIONS PERSONNELLES EXCESSIVES

13 Les institutions de l'UE entrent parfois en possession d'informations à caractère personnel manifestement dénuées de tout intérêt ou pertinence au regard des allégations. **Les informations de ce type ne doivent pas faire l'objet d'un traitement ultérieur**. Cette exigence est particulièrement importante pour certaines catégories d'informations. Tous les agents chargés de l'examen des allégations doivent être informés de cette règle.

> ***Exemple 2:*** *un lanceur d'alerte signale qu'un de ses collègues a effectué une activité frauduleuse. Dans le cadre de sa déclaration, il se retrouve à divulguer des informations sur l'état de santé de son collègue. Il est clair, pour l'institution, que cette information est complètement dénuée de toute pertinence au regard de l'activité frauduleuse et qu'elle ne doit donc ni faire l'objet d'un traitement ultérieur, ni être renvoyée à son expéditeur.*

[4] Article 4, paragraphe 1, point b), du règlement.
[5] Article 10, paragraphe 1, du règlement.

14 Il est de bonne pratique d'émettre une recommandation générale à l'intention des personnes chargées de traiter les dossiers, par exemple dans le règlement intérieur de procédure, leur rappelant les exigences en matière de qualité des données[6] et leur recommandant de veiller au respect des règles.

5. DÉTERMINER CE QUE LE TERME «INFORMATIONS À CARACTÈRE PERSONNEL» SIGNIFIE DANS CE CONTEXTE

15 Les données à caractère personnel sont définies comme toute information concernant une personne physique identifiée ou identifiable[7]. Les informations à caractère personnel n'incluent pas seulement les informations relatives à la vie privée et familiale d'un individu, mais aussi les informations concernant les activités d'une personne, telles que ses relations professionnelles ou son comportement économique et social[8]. Il convient de prendre en compte ces éléments lors de la détermination de la portée du droit d'accès de la personne concernée. La plupart du temps, les informations à caractère personnel incluent des données d'identification (coordonnées, etc.), mais aussi des informations relatives au comportement de l'individu.

Exemple 3: *le rapport du lanceur d'alerte inclut des informations identifiant le présumé responsable et les témoins. Il contient également des informations personnelles sur le lanceur d'alerte, puisqu'il concerne son propre comportement (en tant que lanceur d'alerte).*

16 Une même information peut concerner plusieurs individus en même temps. Le rapport du lanceur d'alerte peut contenir des informations à caractère personnel sur les témoins et tierces parties (des personnes uniquement citées dans le dossier), les personnes à l'encontre desquelles les allégations sont portées et le lanceur d'alerte lui-même.

17 Par contre, le seul fait qu'un nom soit mentionné dans un document ne fait pas nécessairement de toutes les informations qui y figurent des «données relatives à cette personne». Dans bon nombre de cas, une information ne peut être considérée comme «relative à» un individu que si elle concerne celui-ci.

Exemple 4: *une institution de l'UE rédige un rapport dans lequel elle examine la pertinence d'un renvoi de l'affaire devant l'OLAF. Dans son analyse, elle peut faire référence au lanceur d'alerte en tant que source, mais le rapport n'est pas entièrement constitué d'informations personnelles sur le lanceur d'alerte.*

6. INFORMER CHAQUE CATÉGORIE DE PERSONNES

18 Les informations sur les procédures d'alerte éthique doivent être fournies aux personnes concernées de façon très visible, ce qui nécessite une procédure en **deux temps**. Si

[6] Article 4, paragraphe 1, du règlement.
[7] Article 2, point a), du règlement.
[8] Groupe de travail «Article 29», avis 4/2007 sur le concept de données à caractère personnel, WP 136, adopté le 20 juin 2007.

l'affichage d'une déclaration relative à la protection des données sur le site web (ou sur un document public ou interne) est sans aucun doute une démarche positive, le CEPD considère qu'il **ne suffit pas**, car les informations ne seront pas forcément lues. Une déclaration spécifique relative à la protection des données devrait également être mise directement à la disposition de toutes les personnes impliquées dans une procédure d'alerte éthique, par exemple par courrier électronique. Les personnes concernées sont en général les lanceurs d'alerte, les témoins, des tierces parties (des membres du personnel ou d'autres personnes uniquement citées) ainsi que la ou les personnes visées par les allégations.

6.1. Information du lanceur d'alerte (article 11 du règlement)

19 Dans ce contexte, il importe d'informer le lanceur d'alerte sur les destinataires ou catégories de destinataires potentiels[9] de ses informations à caractère personnel. La déclaration relative à la protection des données doit également informer les personnes des conséquences d'une utilisation abusive (si le lanceur d'alerte effectue une fausse déclaration par malveillance) de la procédure d'alerte éthique (p.ex. des mesures disciplinaires).

6.2. Informations fournies au présumé responsable

20 Dans certains cas, informer la personne à l'encontre de laquelle une allégation a été portée à un stade précoce de la procédure peut compromettre le bon déroulement de celle-ci. Dans ce type de cas, il peut être nécessaire de différer le partage de certaines informations spécifiques.[10] Le report de l'information devrait être décidé au cas par cas. Les raisons des éventuelles limitations doivent être documentées et mises à la disposition du CEPD s'il en fait la demande dans le cadre d'une mesure de surveillance et d'application. Ces raisons doivent démontrer, par exemple, l'existence d'un risque élevé que l'accès aux informations nuise à la procédure ou aux droits et libertés des autres personnes. Les raisons doivent être documentées avant l'adoption de la décision relative à d'éventuelles limitations ou à un renvoi.

6.3. Information des témoins (article 11 du règlement)

21 Des informations spécifiques doivent être fournies aux témoins dans les plus brefs délais, par exemple avant qu'ils soient interrogés par l'institution.

6.4. Information des tierces parties (article 12 du règlement)

22 Selon le cas particulier, l'information de toutes les tierces parties mentionnées dans un rapport d'alerte éthique peut supposer un effort disproportionné[11]. Il convient de déterminer au cas par cas si l'information des tierces parties est disproportionnée. Par ailleurs, dans certains cas, l'information des personnes représenterait un traitement supplémentaire potentiellement plus intrusif que le premier.

[9] Article 11, paragraphe 1, point c), du règlement.
[10] Article 20 du règlement.
[11] Article 12, paragraphe 2, du règlement.

Exemple 5:
a) un lanceur d'alerte joint à son rapport une liste des clients (200 personnes) d'un hôtel afin de prouver que le présumé responsable se trouvait à l'hôtel à une date donnée. Les 199 autres clients n'ont aucun lien avec l'affaire et leurs informations ne font pas l'objet d'un traitement ultérieur par l'institution. Il n'est pas nécessaire de les informer.
b) Un lanceur d'alerte joint à son rapport une clé USB contenant des échanges de courriers électroniques avec le présumé responsable et quelques autres membres du personnel. L'institution effectue un examen préliminaire et traite les informations relatives aux autres membres du personnel. Il convient alors d'en informer ceux-ci.

7. ÉVALUER LE DROIT D'ACCÈS ET LES LIMITATIONS DE L'ACCÈS DE LA PERSONNE

23 Lorsqu'elles examinent les droits d'accès, les institutions doivent tenir compte du statut du demandeur et de l'état actuel[12] de l'enquête. Le niveau et la sensibilité des informations détenues (ainsi que tout éventuel risque associé à leur divulgation) varient en fonction de l'auteur de la demande:

- la personne visée par une allégation;
- le lanceur d'alerte;
- un témoin;
- une tierce partie.

24 Les institutions doivent évaluer au cas par cas chaque affaire et documenter les raisons justifiant leur décision, en tenant compte du type d'informations détenues et de l'éventuelle application d'exceptions au règlement.

25 **Lorsque l'accès aux informations personnelles d'un individu est accordé, les informations à caractère personnel de tierces parties telles que des informateurs, des lanceurs d'alerte ou des témoins doivent être effacées des documents, sauf dans des circonstances exceptionnelles,** si le lanceur d'alerte consent à cette divulgation, pour les besoins d'une éventuelle procédure pénale ultérieure ou en cas de fausse déclaration du lanceur d'alerte effectuée par malveillance. Si un risque d'identification de tierces parties subsiste, l'accès doit être reporté. Le groupe de travail «Article 29» recommande ce qui suit: «*la personne accusée dans le rapport d'un dénonciateur ne peut en aucune circonstance obtenir du système des informations concernant l'identité du dénonciateur (...), sauf lorsque le dénonciateur fait une fausse déclaration par malveillance.Dans tous les autres cas, la confidentialité de l'identité du dénonciateur doit toujours être garantie*».[13] Cette recommandation est particulièrement importante si l'on veut faire en sorte que les individus soient protégés contre tous les risques potentiels inhérents à la divulgation de leurs informations à caractère personnel.

[12] Voir l'article 20, paragraphe 1, point a), du règlement.
[13] Avis du groupe de travail «Article 29» relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, WP 117, adopté le 1er février 2006, p. 14

Exemple 6: *un employé de l'UE accusé de manquements graves demande à l'institution toutes les informations à caractère personnel le concernant en rapport avec les accusations. La plupart de ces informations figurent dans les témoignages du lanceur d'alerte. Même si le nom de celui-ci est effacé des documents, son identité serait évidente au vu des références aux évènements, situations et contextes spécifiques qui y sont décrits. L'institution doit donc différer la publication de ces informations pour garantir la protection de la personne concernée ou des droits et libertés d'autrui (article 20, paragraphe 1, point c)).*

8. LIMITER LES TRANSFERTS

26 Différentes obligations s'appliquent selon que le destinataire est une institution de l'UE (dans ce contexte, lorsqu'une institution transfère des données à l'OLAF) ou une entité soumise à la directive 95/46 (comme une juridiction nationale ou un autre type de destinataire).[14] **La nécessité de ce transfert de données doit être déterminée au cas par cas**. En particulier, le transfert de données à caractère personnel n'est justifié que lorsqu'il est nécessaire à l'exécution légitime des missions relevant de la compétence du destinataire.

9. ÉTABLIR DES PÉRIODES DE CONSERVATION EN FONCTION DE L'ISSUE DE L'AFFAIRE

27 Les informations à caractère personnel peuvent uniquement être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées.[15] Il convient donc de fixer différentes périodes de conservation en fonction des informations incluses dans le rapport et de la manière dont l'affaire est traitée.

28 Premièrement, comme indiqué ci-dessus, les informations à caractère personnel qui ne sont pas pertinentes au regard des allégations ne peuvent être traitées (voir le point 4).

29 Deuxièmement, lorsqu'un examen initial est effectué, mais qu'il apparaît clairement que l'affaire ne devrait pas être renvoyée devant l'OLAF ou qu'elle ne relève pas de la procédure d'alerte éthique, le rapport doit être supprimé dans les plus brefs délais (ou renvoyé vers la bonne filière s'il porte par exemple sur une accusation de harcèlement). En tout état de cause, les informations à caractère personnel devraient être supprimées rapidement et généralement dans un délai de deux mois à compter de l'aboutissement de l'évaluation préliminaire[16], vu que la conservation de telles informations sensibles serait excessive.

30 Troisièmement, s'il apparaît nécessaire, à l'issue de l'examen initial, de transférer le rapport à l'OLAF, l'institution de l'UE doit rester attentive aux mesures que l'OLAF décide de prendre. Si l'OLAF ouvre une enquête, il n'est pas nécessaire que les institutions de l'UE conservent plus longtemps les informations. Si l'OLAF décide de ne pas ouvrir d'enquête, les informations doivent être effacées sans délai.

[14] Articles 7, 8 et 9 du règlement.
[15] Article 4, paragraphe 1, point e), du règlement.
[16] Avis 1/2006 du Groupe de travail «Article 29», WP 117, p. 12.

31 Dans le cas où une période de conservation plus longue serait envisagée, l'accès aux informations à caractère personnel doit tout de même être limité (voir les mesures de sécurité ci-dessous). Il est de bonne pratique de conserver ces rapports à l'écart du principal système de gestion des dossiers/système quotidien utilisé.

Exemple 7: *une institution de l'UE a reçu plusieurs rapports d'alerte éthique par le biais de sa filière d'alerte. L'un d'entre eux concerne une accusation de harcèlement et est donc directement renvoyé vers l'unité responsable de ces affaires. Deux autres pourraient porter sur des cas de fraude et sont donc transférés à l'OLAF, qui ouvre une enquête sur l'un des cas. L'institution applique une période de conservation de cinq ans en ce qui concerne les rapports pour lesquels l'OLAF n'ouvre pas d'enquête. Dans cette situation, le CEPD estime qu'une période de cinq ans est excessive et que le rapport devrait être supprimé le plus tôt possible.*

10. METTRE EN ŒUVRE DES MESURES DE SÉCURITÉ ADÉQUATES

32 Le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles adéquates pour assurer un niveau de sécurité approprié aux risques présentés par le traitement et à la nature des informations personnelles à traiter[17]. Il ne s'agit pas seulement d'une exigence juridique clairement établie, puisque, comme déjà mentionné, la confidentialité de l'ensemble de la procédure est capitale pour encourager le personnel à signaler tous les doutes qu'il pourrait avoir. Les mesures de sécurité doivent en outre prendre en considération le caractère sensible des informations personnelles traitées. Il est essentiel, dans ce contexte, de mettre en place des mesures de sécurité adéquates afin d'empêcher efficacement les personnes non autorisées d'accéder aux informations à caractère personnel et de garantir l'intégrité de celles-ci.

33 **La nécessité de ces mesures de sécurité doit être analysée à la lumière des risques inhérents à la procédure d'alerte éthique**, que celle-ci soit manuelle ou automatisée, en effectuant une **évaluation des risques pour la sécurité des informations**. Une fois que les risques pour les informations à caractère personnel concernées ont été déterminés, une nouvelle analyse peut être effectuée afin de déterminer les mesures à mettre en œuvre, en tenant également compte du coût de ces mesures de sécurité et de leur viabilité. Les risques évoluant au fil du temps, il est nécessaire que l'institution de l'UE réexamine régulièrement son analyse, la sélection des mesures de sécurité ainsi que l'efficacité de celles-ci.

34 Des orientations détaillées sur la gestion des risques relatifs à la sécurité des informations sont proposées dans le document «Guidance on Security Measures for Personal Data Processing - Article 22 of Regulation 45/2001».

[17] Voir l'article 22 du règlement.

Exemple 8: *en particulier lorsqu'il s'agit de dossiers d'alerte éthique,*
a) le personnel ayant accès aux informations à caractère personnel doit être strictement limité en fonction du principe du besoin d'en connaître. Le personnel autorisé doit être soumis à une obligation de confidentialité renforcée et l'accès aux rapports d'alerte éthique doit être contrôlé, qu'il se fasse sous forme électronique ou sur papier.
b) Du point de vue technique, les exigences habituelles relatives au contrôle de l'accès doivent être pleinement appliquées, à savoir limiter et contrôler efficacement les personnes autorisées à accéder aux dossiers d'alerte éthique, enregistrer les accès et réexaminer régulièrement les accès et les droits d'accès.
c) Vu l'importance d'assurer une stricte confidentialité de ces informations, il convient d'envisager notamment le recours au cryptage. Même en cas de cryptage, des mécanismes de

11. VEILLEZ À POUVOIR RENDRE DES COMPTES!

35 L'obligation de rendre des comptes signifie que les organisations doivent respecter leurs obligations en matière de protection des données et **être en mesure de démontrer qu'elles le font**.

36 Cette notion n'est pas propre aux informations à caractère personnel concernées par une procédure d'alerte éthique, mais s'applique à toutes les opérations de traitement d'informations à caractère personnel.

37 Toute organisation qui collecte, utilise et stocke (ce que l'on appelle collectivement le traitement) des informations à caractère personnel est responsable du respect des règles en matière de protection des données et doit pouvoir rendre des comptes à cet égard.

38 D'une manière générale, les institutions doivent faire preuve de transparence et être explicites quant à la manière dont elles traitent les informations à caractère personnel liées aux procédures d'alerte éthique. Elles doivent documenter leurs politiques et veiller à ce que les utilisateurs en aient connaissance. Le droit au respect de la vie privée existe sur le lieu de travail également et tout le monde doit en être informé. Les institutions ne peuvent pas partir du principe que le personnel est au courant.

39 Le meilleur moyen pour une institution de pouvoir rendre des comptes consiste à examiner les implications des nouveaux processus du point de vue de la protection des données dès le stade de la conception (**protection des données dès la conception**). Les différents traitements et les différentes technologies exigent des garanties différentes. S'il est associé dès le début du processus, le délégué à la protection des données (DPD) pourra apporter des conseils et des orientations utiles.

40 Les questions figurant ci-après exposent les principaux points à prendre en considération:

a. **Confidentialité:** comment protégez-vous les personnes concernées?
b. **Déterminer la finalité:** quand utiliser la filière d'alerte éthique?
c. **Éviter les informations excessives:** quelles informations sont nécessaires au vu des allégations formulées?

d. **Définir le terme «informations à caractère personnel»:** qu'est-ce qu'une information à caractère personnel dans ce rapport particulier?

e. **Informer chaque catégorie de personnes:** qui sont les personnes affectées par ce rapport particulier?

f. **Appliquer différentes périodes de conservation:** combien de temps dois-je conserver le rapport?

g. **Effectuer une évaluation des risques pour la sécurité des informations:** Quels sont les risques auxquels sont exposés vos cas d'alerte éthique? Comment allez-vous vous en protéger?

41 L'obligation de rendre des comptes suppose également de documenter la procédure et son application. Les éléments suivants doivent être documentés:

a. une **politique, un règlement interne ou une décision** sur l'alerte éthique;

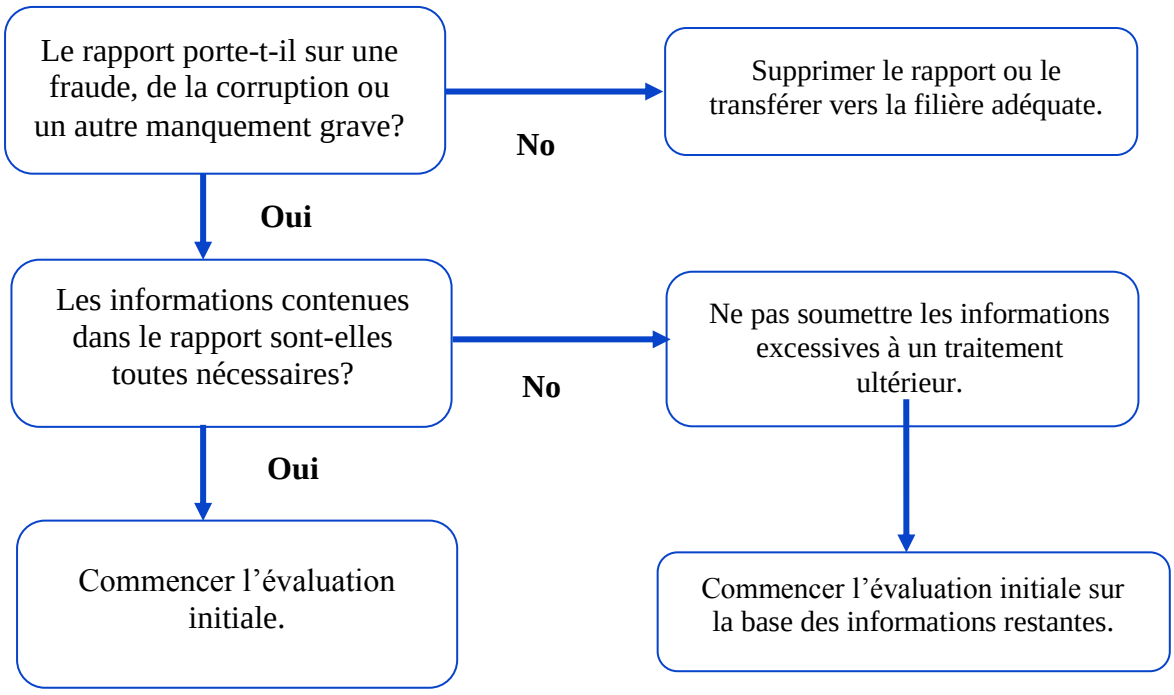
b. **les limitations du droit d'accès** doivent être documentées, en indiquant non seulement les motifs sur lesquels elles reposent, mais aussi le raisonnement utilisé pour justifier leur application à la situation en question;

c. tout **report de l'information** de la personne;

d. l'**évaluation des risques** effectuée pour la procédure en question.

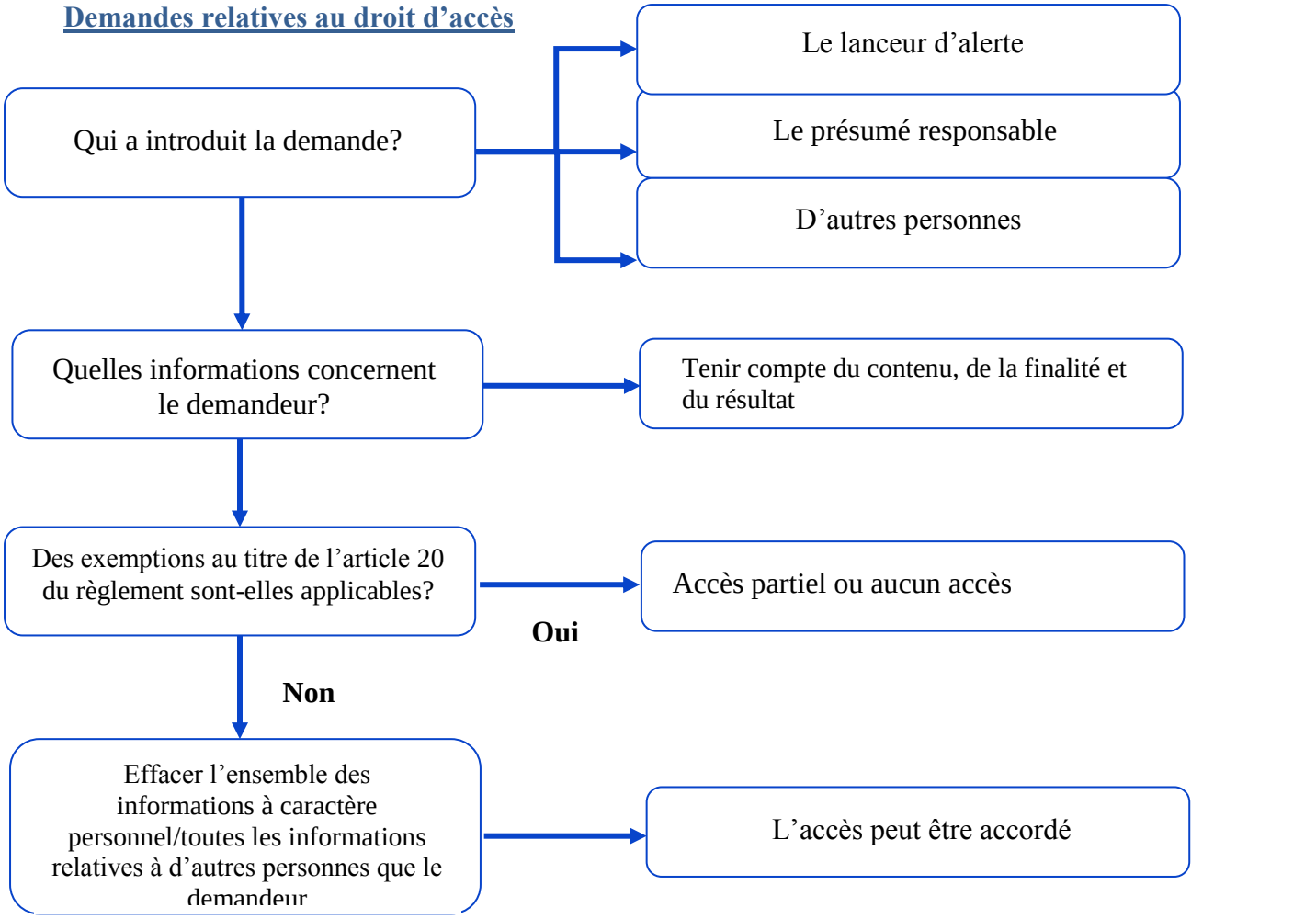
12. ORGANIGRAMMES DES PROCÉDURES D'ALERTE ÉTHIQUE

12.1. Gestion des rapports d'alerte éthique

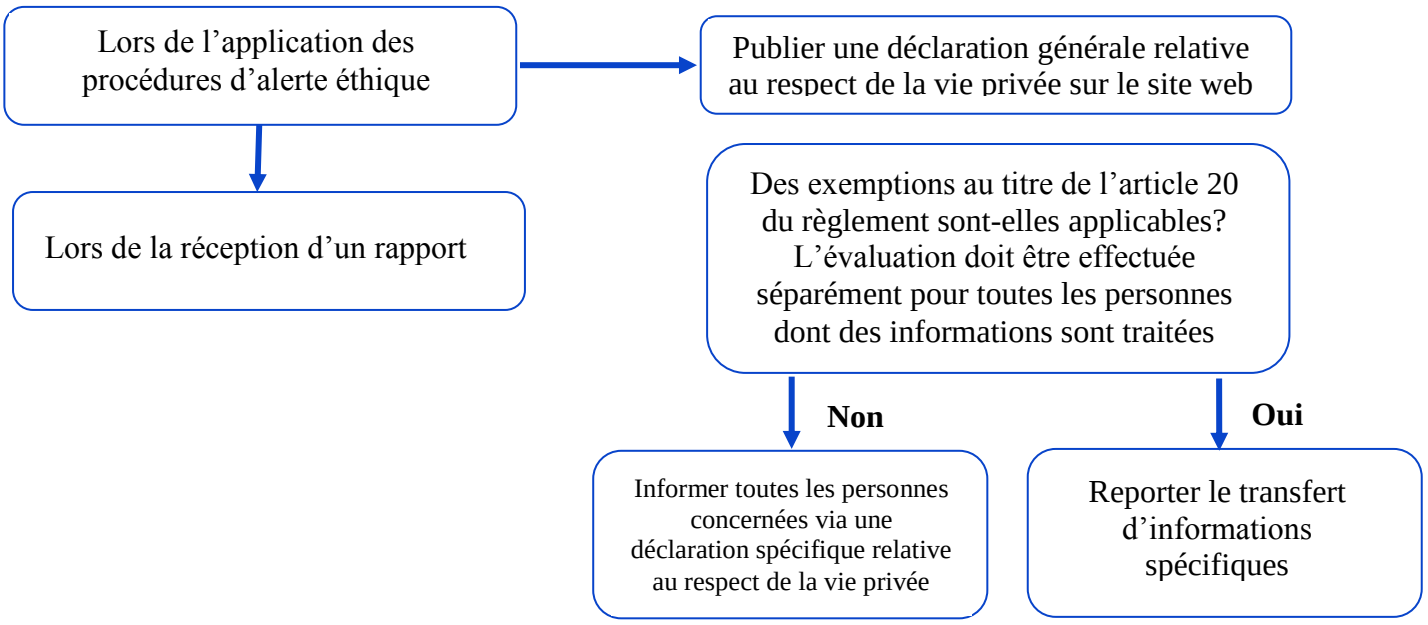


12.2. Garantir le respect des droits des personnes

Demandes relatives au droit d'accès



Comment informer correctement les personnes



LECTURES COMPLÉMENTAIRES

Exemples d'avis du CEPD

2014-0828 - Avis sur la procédure d'alerte éthique du Médiateur européen

2015-0061 - Avis du CEPD sur la procédure de l'Agence exécutive du Conseil européen de la recherche relative au traitement interne et au signalement d'éventuelles fraudes et irrégularités

2015-0349 - Avis sur la procédure d'alerte éthique du Secrétariat général du Conseil de l'Union européenne

2015-0569 - Avis sur la procédure de transmission d'informations de l'Agence européenne de contrôle des pêches

Autres documents

La protection des lanceurs d'alerte - recommandation CM/Rec(2014)7 - Conseil de l'Europe

Whistleblowing in Europe, legal protection for whistleblowers in the EU - Transparency National International principles for whistleblower legislation - Transparency National